UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,948	03/23/2004	Bruce Wayne Yancy	GCSD-1575 (51397)	2885

74701 7590 05/20/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
05/20/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/806,948	YANCY ET AL.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 1/24/2008. Claims 1-41 were received for consideration.

Response to Arguments

Applicant's arguments with respect to the combination of Dellmo and Stalling have been fully considered but they are not persuasive. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN, as taught in Stallings, since it thwarts traffic analysis based on ultimate destination with the network interface of Dellmo.

Applicant's arguments with respect to Dichter not teaching said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices have been fully considered but they are not persuasive. Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 1 and column 1 lines 30-34).

Applicant's arguments with respect to the combination of Dellmo and Dichter have been fully considered but they are not persuasive. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 3, 4, 9, 10, 21, 23-25, 26, 28, 31, 33-35, 36, 38 39, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices. With respect to claim 1 Dellmo teaches a cryptographic device comprising: a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) and a communications module (paragraph 0038 i.e. wireless transceiver 50) coupled thereto (see figure 7); said cryptographic module comprising a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user network interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said communications module comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices; said network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon.

Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see column 1 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16). Therefore one would have been motivated to have a plurality of different connectors for coupling the cryptographic module to different network devices.

Stallings teaches said network processor (see page 418 lines 8-13 i.e. source prepares an inner IP packet) generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion (see page 418 lines 8-13 i.e. inner IP packet), and encapsulating the command packets for said communication module in the data portions of a communications module command packet (see page 418 lines 8-13 i.e. encapsulated with a new IP header);

said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon (see page 418 lines 8-13 the new IP packet is not encrypted). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN since it thwarts traffic analysis based on ultimate destination. Therefore one would be motivated to have used a VPN.

With respect to claim 3, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to claim 4, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 9, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 10, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see Dellmo figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein said network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 21 Dellmo teaches communications method comprising: coupling a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) to a

network device (see figure 2), the cryptographic module comprising a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to the user network interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to the host network processor (see figure 7); providing a communications module (paragraph 0038 i.e. wireless transceiver 50) comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to the cryptographic processor (see figure 7);

Dellmo does not teach said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices; said network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon.

Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see column 1 lines 30-34). It would have been obvious at the time the invention was made

to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16). Therefore one would have been motivated to have a plurality of different connectors for coupling the cryptographic module to different network devices.

Stallings teaches said network processor (see page 418 lines 8-13 i.e. source prepares an inner IP packet) generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion (see page 418 lines 8-13 i.e. inner IP packet), and encapsulating the command packets for said communication module in the data portions of a communications module command packet (see page 418 lines 8-13 i.e. encapsulated with a new IP header); said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon (see page 418 lines 8-13 the new IP packet is not encrypted). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN since it thwarts traffic analysis based on ultimate destination. Therefore one would be motivated to have used a VPN.

With respect to claim 23, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to 24, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 25, wherein the user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein the network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 26, Dellmo teaches a communications system comprising: a plurality of network devices coupled together to define a network (see figure 4 and paragraph 0035), and a cryptographic device (see figure 2 element 20) coupled to at least one of said network devices (see figure 2); said cryptographic device comprising a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) coupled to said at least one network device (see figure 2), and a communications module (paragraph 0038 i.e. wireless transceiver 50) coupled to said cryptographic module (see figure 7); said cryptographic module comprising a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user network interface (see figure 2), and a cryptographic processor see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said

communications module comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices; said network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon.

Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see column 1 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16). Therefore one would have been motivated to have a plurality of different connectors for coupling the cryptographic module to different network devices.

Stallings teaches said network processor (see page 418 lines 8-13 i.e. source prepares an inner IP packet) generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion (see page 418 lines 8-13 i.e. inner IP packet), and encapsulating the command packets

for said communication module in the data portions of a communications module command packet (see page 418 lines 8-13 i.e. encapsulated with a new IP header); said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon (see page 418 lines 8-13 the new IP packet is not encrypted). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN since it thwarts traffic analysis based on ultimate destination. Therefore one would be motivated to have used a VPN.

With respect to 28. The system of claim 26 wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036), and wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 33, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph Dellmo 0035 and 0041-0046).

With respect to claim 34, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein said network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 35, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see Dellmo paragraph 0060).

With respect to claim 36 Dellmo teaches, a cryptographic module comprising: a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices); a host network processor see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device) coupled to said user network interface (see figure 2); and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7);

Dellmo does not teach said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices; said network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon.

Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see

column 1 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16). Therefore one would have been motivated to have a plurality of different connectors for coupling the cryptographic module to different network devices.

Stallings teaches said network processor (see page 418 lines 8-13 i.e. source prepares an inner IP packet) generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion (see page 418 lines 8-13 i.e. inner IP packet), and encapsulating the command packets for said communication module in the data portions of a communications module command packet (see page 418 lines 8-13 i.e. encapsulated with a new IP header); said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon (see page 418 lines 8-13 the new IP packet is not encrypted). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN since it thwarts traffic analysis based on ultimate destination. Therefore one would be motivated to have used a VPN.

With respect to claim 38, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to 39, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 41, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices).

Claim 2, 22, 26, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in further view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols". Dellmo Dichter and Stalings teach everything with respect to claim 1, 21, 26 and 36 above but with respect to claim 2, 22, 26, and 37 they do not teach wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP). Stevens teaches wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP) (see Stevens page 359). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Simple Network Management Protocol to help manage the network (see page 359). Therefore one would have been motivated to have used Simple Network Management Protocol.

Claims 5, 6, 8, 11, 29, 30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in further view of Cheng (U.S. 2003/0221034). Dellmo Dichter and Stalings teach everything with respect to claim 1, and 26 above but with respect to claim 5, 6, 29 and 30 they do not teach wherein said cryptographic module further comprises: a first housing carrying said user network interface, said host network processor, said cryptographic processor; and a first connector carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing carrying said network communications interface; and a second connector carried by said second housing and being removable mateable with said first connector of said cryptographic module. Cheng teaches wherein said cryptographic module further comprises: a first housing (see Cheng figure 4 element 51A) carrying said user network interface, said host network processor, said cryptographic processor; and a first connector (see Cheng figure 4 element 53A) carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing (see Cheng figure 4 element 51B) carrying said network communications interface; and a second connector (see Cheng figure 4 element 53B) carried by said second housing and being removable mateable with said first connector of said cryptographic module (see Cheng figure 4). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have made the communications module removable coupled

with the cryptographic module to allow the user to change the module based on changing requirements (see paragraph 0030). Therefore one would have been motivated to have made the communications module removable coupled with the cryptographic module.

With respect to claim 8, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

With respect to claim 11, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see Dellmo paragraph 0060).

With respect to claim 32, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

Claims 7, 31 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in further view of Hashimoto (U.S. 4,907,275). Dellmo Dichter and Stalings teach everything with respect to claim 1, 26 and 36 above but with respect to claim 7, 31 and 40 they do not teach wherein said cryptographic processor comprises: an unencrypted data buffer circuit

coupled to said host network processor; a cryptography circuit coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit coupled to said cryptography circuit. Hashimoto teaches wherein said cryptographic processor comprises: an unencrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said host network processor (see Hashimoto figure 2B element 12); a cryptography circuit (see Hashimoto figure 2B element 15) coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said cryptography circuit. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted data buffer circuit and an unencrypted data buffer circuit to help control the data flow into and out of the cryptography circuit. (see column 3 line 57 – column 4 line 2). Therefore one would have been motivated to have an encrypted data buffer circuit coupled between said user network interface and said cryptography circuit; and an unencrypted data buffer circuit coupled between said cryptography circuit and said network communications interface.

Claims 12, 13, and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in further view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols". Dellmo Dichter and Stalings teaches with respect to claim 12, a cryptographic device comprising: a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) and a

communications module (paragraph 0038 i.e. wireless transceiver 50) coupled thereto (see figure 7); said cryptographic module comprising a user Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user LAN interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said communications module comprising a network LAN interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices; said host network processor generating a Ethernet command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating Ethernet command packets for said communications module in the data portions of a cryptographic processor command packets, said host network processor formatting the data portions based upon the simple network management protocol (SNMP); said cryptographic processor passing the communications module command packets to said communications module without performing cryptographic processing thereon.

Dichter teaches said user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices (see

column 1 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a plurality of different connectors coupled to a hub (cryptographic module) to allow different computer to connect to the device (see Dichter column 1 lines 11 – column 2 line 16). Therefore one would have been motivated to have a plurality of different connectors for coupling the cryptographic module to different network devices.

Stallings teaches said host network processor (see page 418 lines 8-13 i.e. source prepares an inner IP packet) generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion (see page 418 lines 8-13 i.e. inner IP packet), and encapsulating Ethernet command packets for said communications module in the data portions of a cryptographic processor command packets (see page 418 lines 8-13 i.e. encapsulated with a new IP header), said cryptographic processor passing the cryptographic processor command packets to said communications module without performing cryptographic processing thereon (see page 418 lines 8-13 the new IP packet is not encrypted). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used VPN since it thwarts traffic analysis based on ultimate destination. Therefore one would be motivated to have used a VPN. Stevens teaches wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP) (see Stevens page 359). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to

have used Simple Network Management Protocol to help manage the network (see page 359). Therefore one would have been motivated to have used Simple Network Management Protocol.

With respect to claim 13 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 18, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 19, wherein said user LAN interface comprises an Ethernet interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices).

With respect to claim 20, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see paragraph 0060).

Claims 14, 15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols" in further view of Cheng (U.S. 2003/0221034). Dellmo, Stalings Dichter and Stevens teach everything with respect to

claim 12 above but with respect to claim 14 and 15 they do not teach wherein said cryptographic module further comprises: a first housing carrying said user network interface, said host network processor, said cryptographic processor; and a first connector carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing carrying said network communications interface; and a second connector carried by said second housing and being removable mateable with said first connector of said cryptographic module. Cheng teaches wherein said cryptographic module further comprises: a first housing (see Cheng figure 4 element 51A) carrying said user network interface, said host network processor, said cryptographic processor; and a first connector (see Cheng figure 4 element 53A) carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing (see Cheng figure 4 element 51B) carrying said network communications interface; and a second connector (see Cheng figure 4 element 53B) carried by said second housing and being removable mateable with said first connector of said cryptographic module (see Cheng figure 4). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have made the communications module removable coupled with the cryptographic module to allow the user to change the module based on changing requirements (see paragraph 0030). Therefore one would have been motivated to have made the communications module removable coupled with the cryptographic module.

With respect to claim 17, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Stalings Cryptography and Network Security Principles and Practices in view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols" in further view of Hashimoto (U.S. 4,907,275). Dellmo, Dichter, Stalings and Stevens teach everything with respect to claim 12 above but with respect to claim 16 they do not teach wherein said cryptographic processor comprises: an unencrypted data buffer circuit coupled to said host network processor; a cryptography circuit coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit coupled to said cryptography circuit. Hashimoto teaches wherein said cryptographic processor comprises: an unencrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said host network processor (see Hashimoto figure 2B element 12); a cryptography circuit (see Hashimoto figure 2B element 15) coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said cryptography circuit. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted data buffer circuit and an unencrypted data buffer circuit to help control the data flow into and out of the cryptography circuit. (see column 3 line 57 – column 4 line 2). Therefore one would

have been motivated to have an encrypted data buffer circuit coupled between said user network interface and said cryptography circuit; and an unencrypted data buffer circuit coupled between said cryptography circuit and said network communications interface.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/
Patent Examiner
4/28/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132